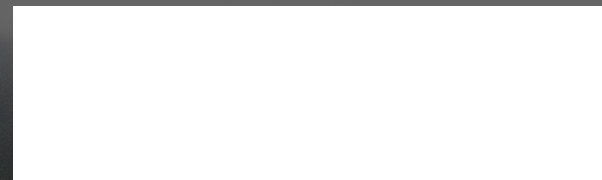
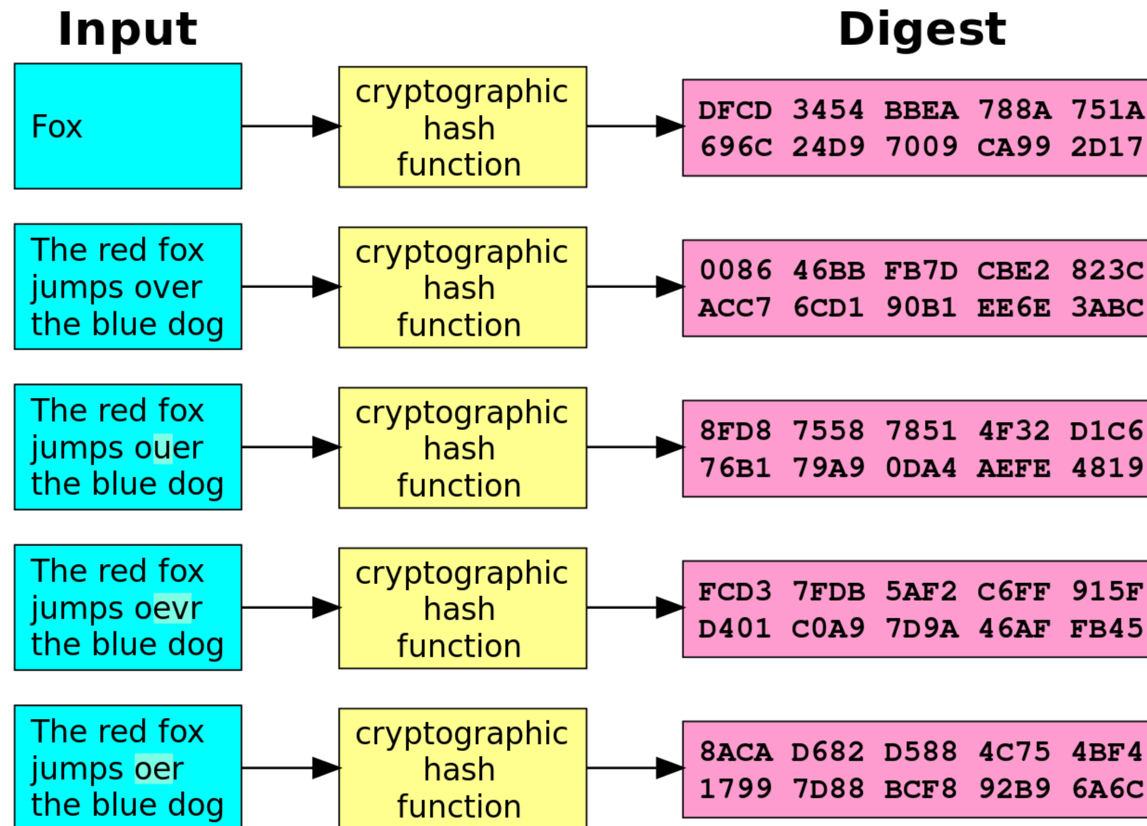
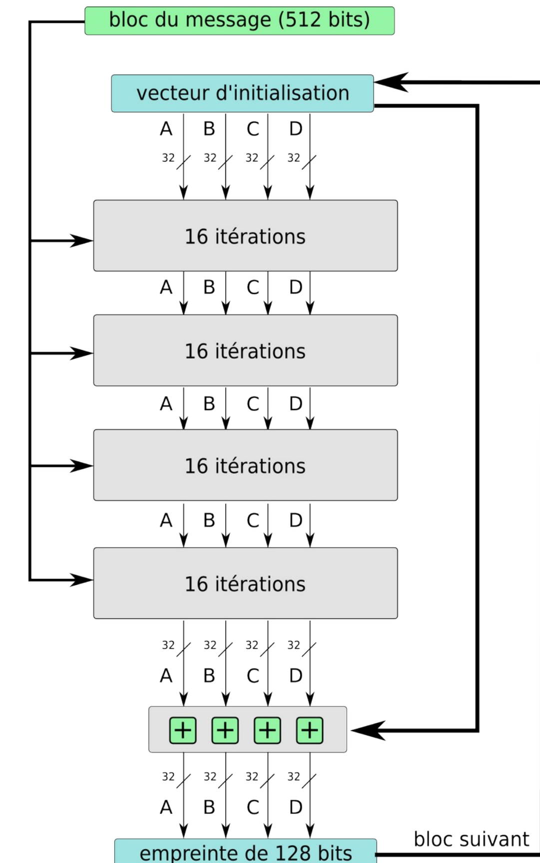


Криптография

Обзор курса

Криптография.





Чего **не** будет в курсе?

Математика

Криптоанализ примитивов и схем

Создание собственных криптографических примитивов и схем

В этом видео

1. Что ожидать от данного курса?
2. Обзор криптографических примитивов
3. Назначение криптографических примитивов

Цели курса

Понять как применяются криптографические примитивы и какими свойствами они обладают

Понимать вектора атак на криптографические схемы

Научиться использовать уязвимости в криптографических схемах

Условные «уровни» в криптографии



GeekBrains

Условные «уровни» в криптографии

Примитив
ы

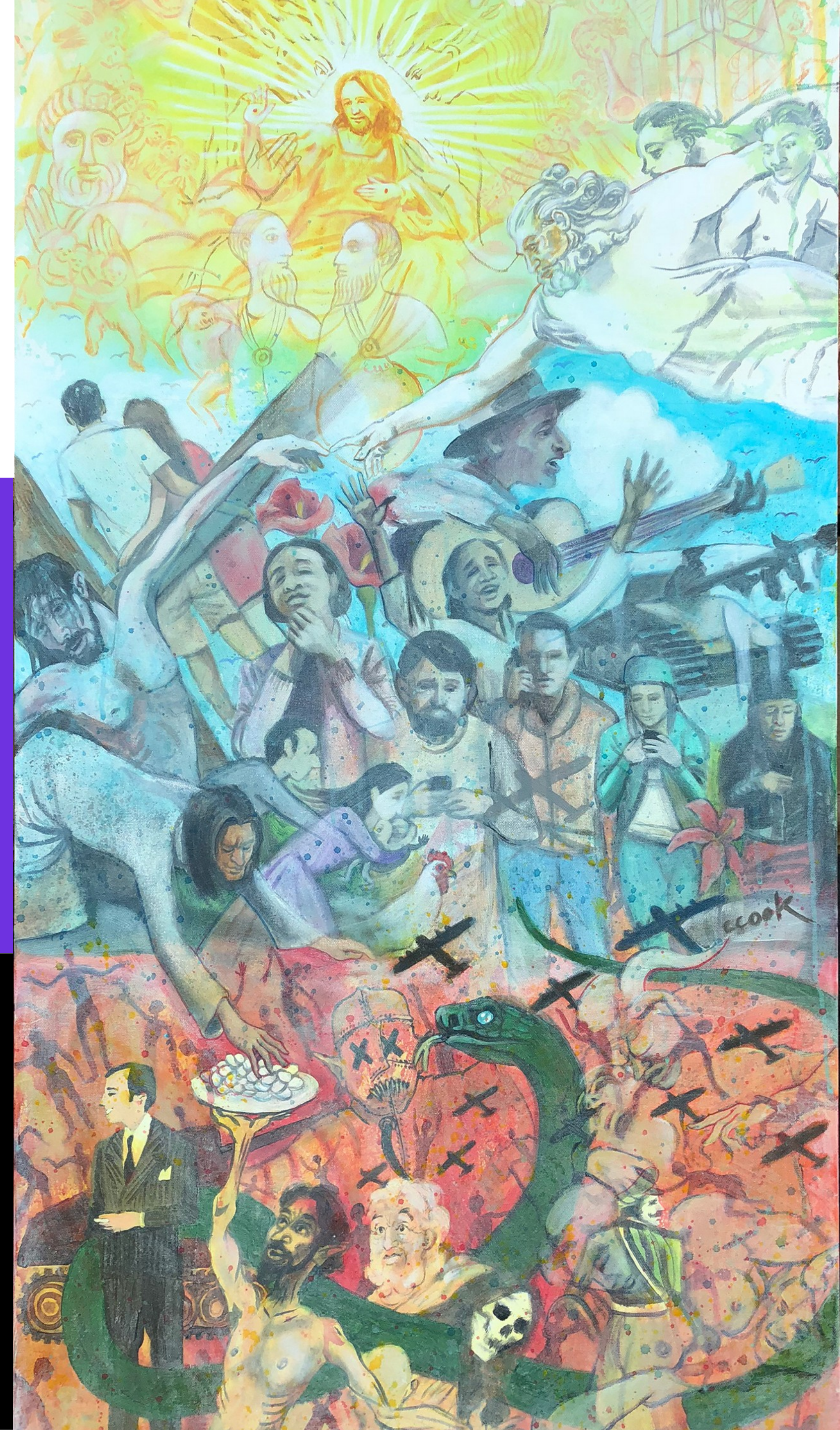
GeekBrains



Условные «уровни» в криптографии

Схемы

Примитивы

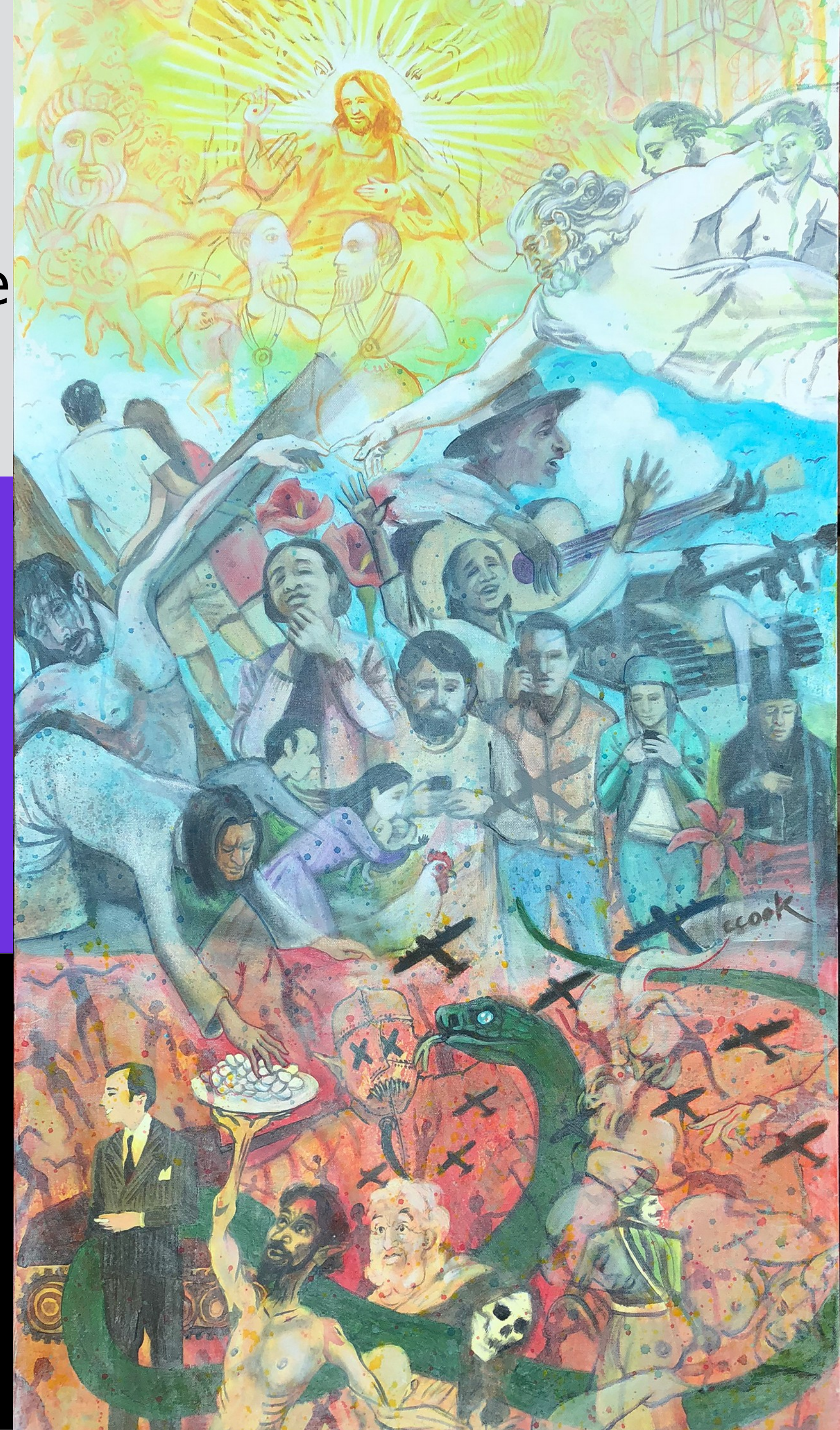


Условные «уровни» в криптографии

Прозрачное применение

Схемы

Примитивы

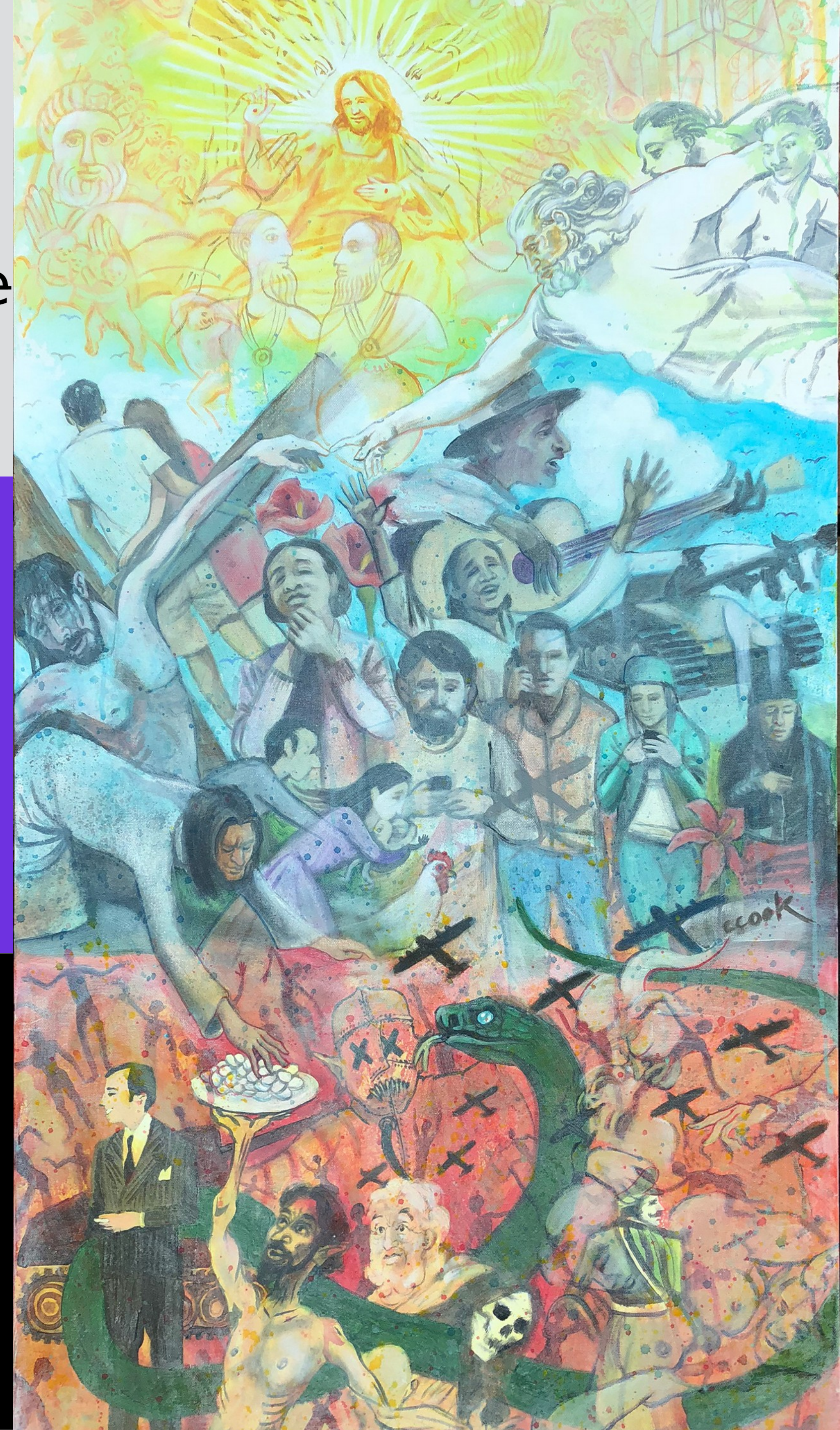


Условные «уровни» в криптографии

~~Прозрачное применение~~

Схемы

~~Примитивы~~



Симметричная криптография (шифр, криптосистема, ...) — криптосистема, в которой шифрование и дешифрование происходит с помощью *одного и того же ключа*.



Крипто… что?

Основные примитивы

Симметричная криптография



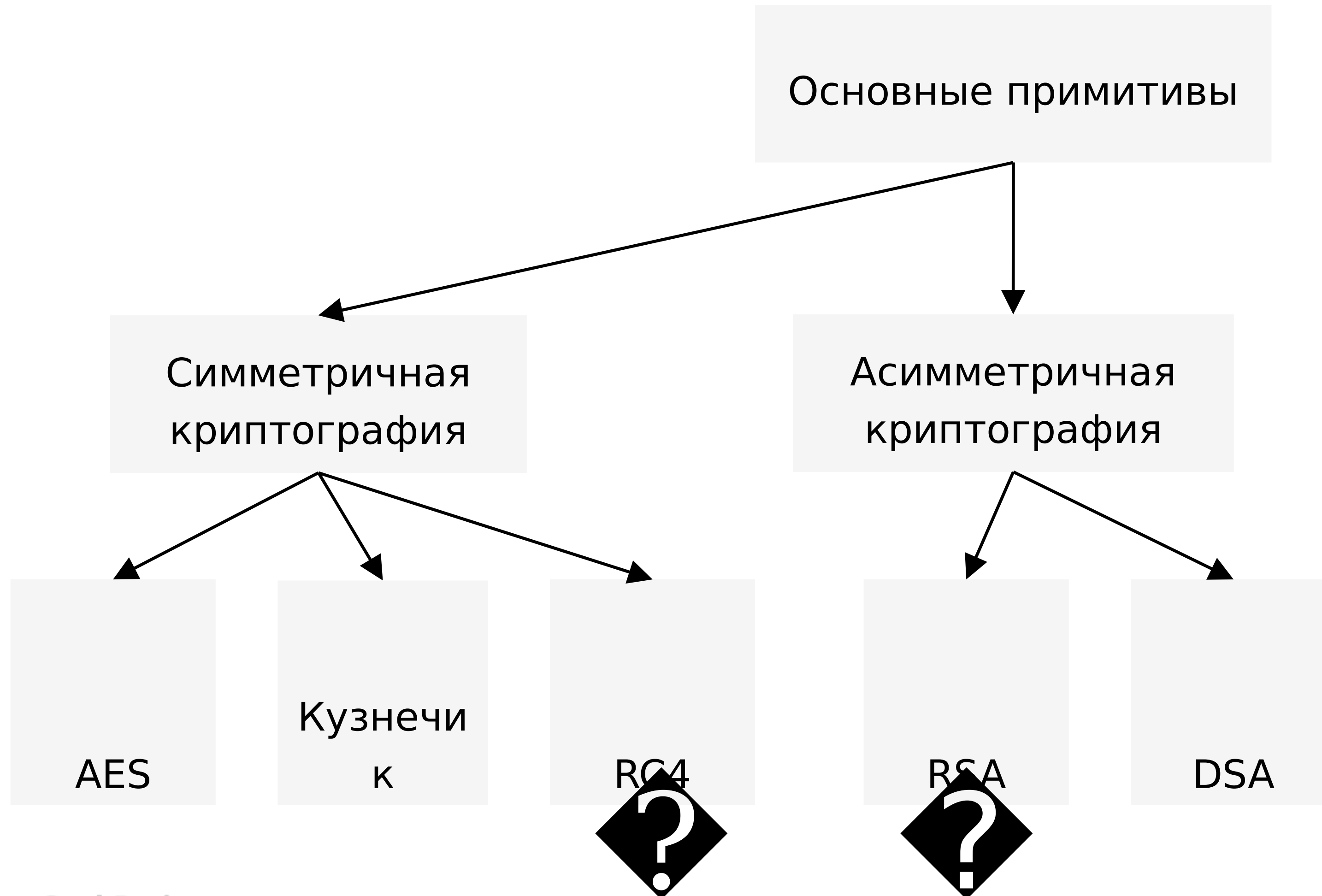
GeekBrains

Асимметричная криптография (шифр, криптосистема, ...) — криптосистема, в которой шифрование и дешифрование происходит с помощью *пары разных ключей* (открытый и закрытый).



GeekBrains

Крипто... что?



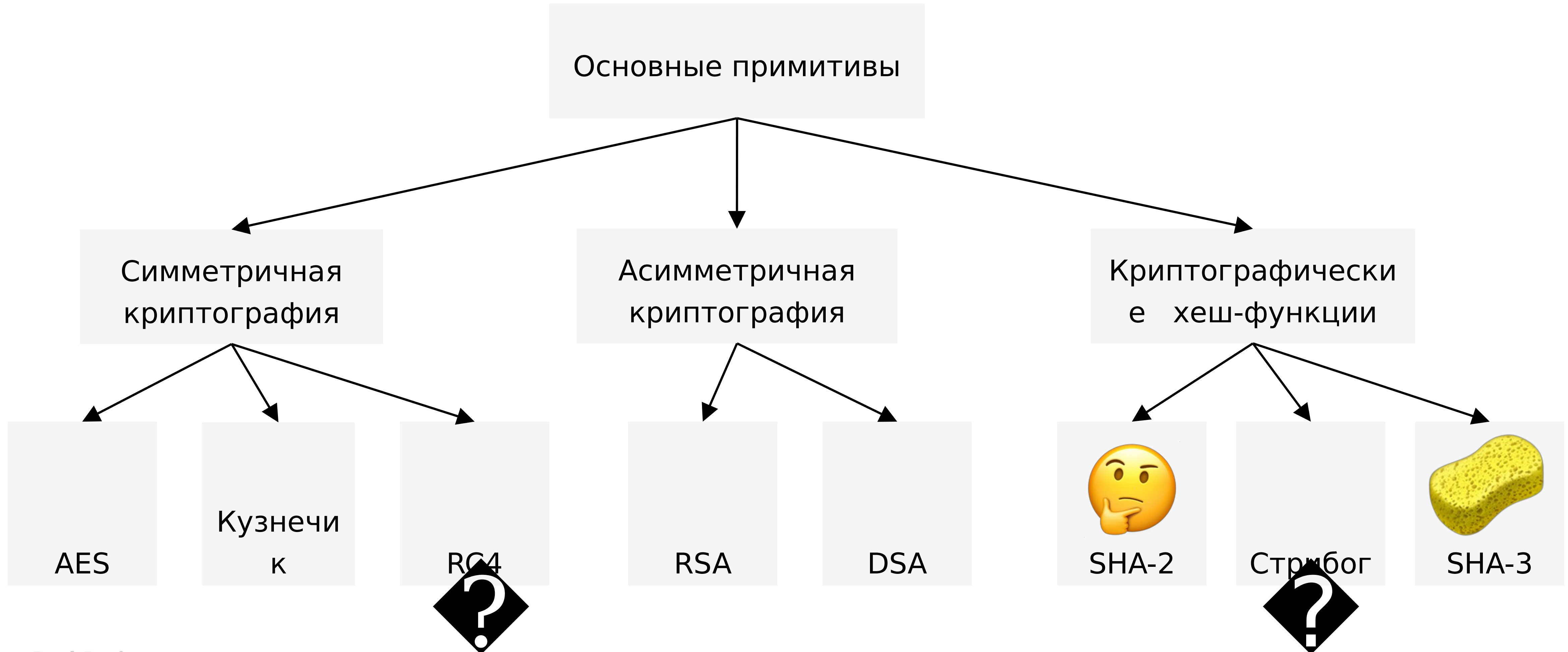
Основные примитивы
Симметричная криптография
Асимметричная криптография
AES
Кузнечик
RC4
RSA
DSA

Криптографическая хеш-функция — функция, которая превращает произвольную строку (данные) в строку фиксированной длины (*с определенными свойствами!*).





Крипто... что?



GeekBrains

Итоги

1. Сформировали цель курса
2. Узнали о криптографических примитивах
3. Поняли для чего может применяться каждый из криптографических примитивов